Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2663644 A1 2008/04/17

(21) 2 663 644

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2007/10/05
(87) Date publication PCT/PCT Publication Date: 2008/04/17
(85) Entrée phase nationale/National Entry: 2009/03/17
(86) N° demande PCT/PCT Application No.: US 2007/080525
(87) N° publication PCT/PCT Publication No.: 2008/045773
(30) Priorités/Priorities: 2006/10/10 (US60/850,882);
2007/10/03 (US11/866,946)

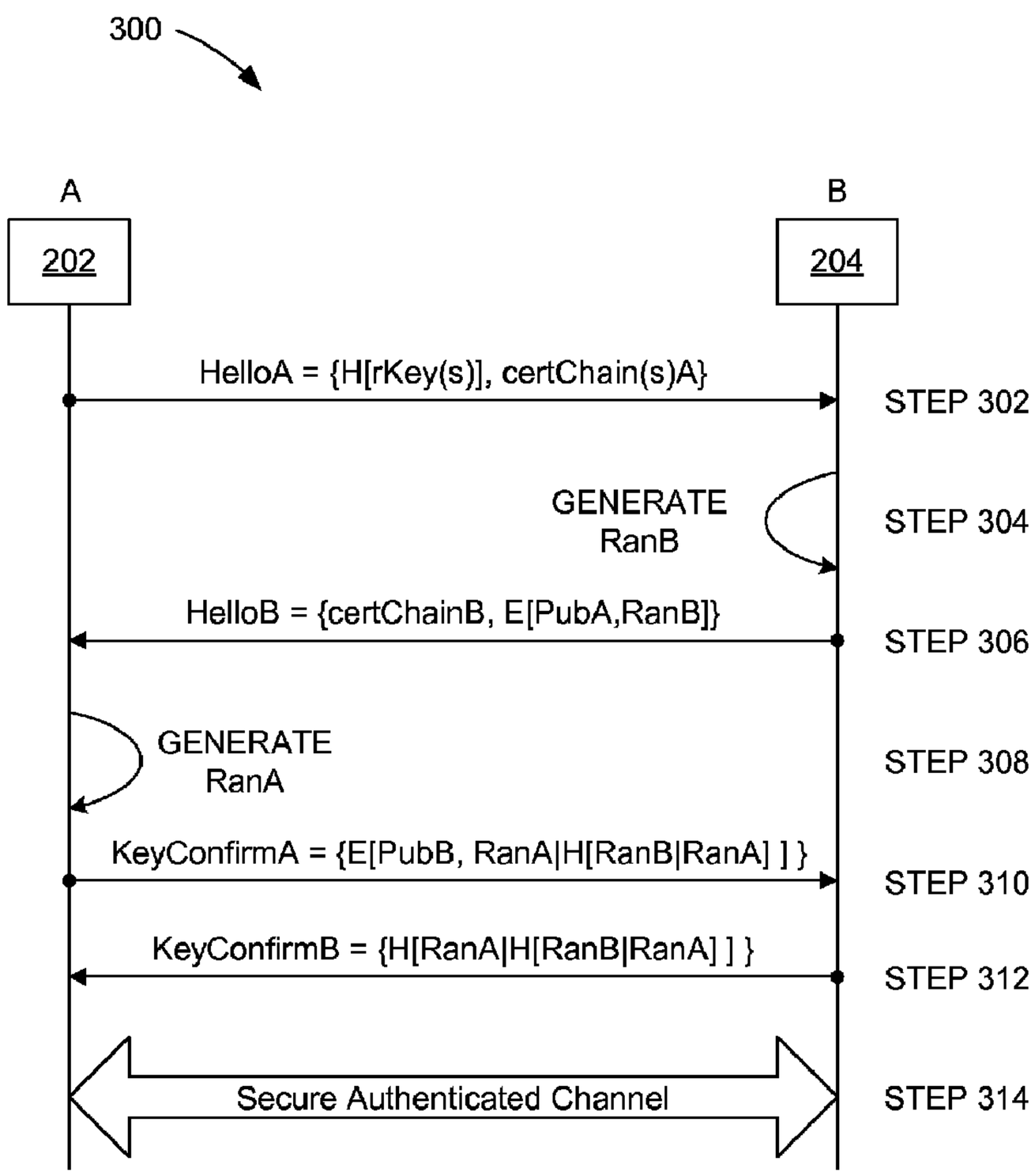
(51) Cl.Int./Int.Cl. *H04L 9/32* (2006.01)

(71) Demandeur/Applicant:
QUALCOMM INCORPORATED, US

(72) Inventeurs/Inventors:
PEREZ, ARAM, US;
DONDETI, LAKSHMINATH REDDY, US

(74) Agent: SMART & BIGGAR

(54) Titre : PROCEDE ET APPAREIL D'AUTHENTIFICATION MUTUELLE
(54) Title: METHOD AND APPARATUS FOR MUTUAL AUTHENTICATION




(57) Abrégé/Abstract:
Disclosed is a method for mutual authentication between a station, having a digital rights agent, and a secure removable media device. The digital rights agent initiates mutual authentication by sending a message to the secure removable media device. The

(21) 2 663 644

(13) A1

(57) Abrégé(suite)/Abstract(continued):
secure removable media device encrypts a first random number using a public key associated with the digital rights agent. The digital rights agent decrypts the encrypted first random number, and encrypts a second random number and a first hash based on at least the first random number. The secure removable media device decrypts the encrypted second random number and the first hash, verifies the first hash to authenticate the digital rights agent, and generates a second hash based on at least the second random number. The digital rights agent verifies the second hash to authenticate the secure removable media device.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 April 2008 (17.04.2008)

PCT

(10) International Publication Number
WO 2008/045773 A3

(51) International Patent Classification:
*H04L 9/32* (2006.01)

(21) International Application Number:
PCT/US2007/080525

(22) International Filing Date: 5 October 2007 (05.10.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

| | | |
|---|---|---|
| 60/850,882 | 10 October 2006 (10.10.2006) | US |
| 11/866,946 | 3 October 2007 (03.10.2007) | US |

(71) Applicant *(for all designated States except US)*: **QUALCOMM Incorporated** [US/US]; Attn: International Ip Administration, 5775 Morehouse Drive, San Diego, California 92121 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **PEREZ, Aram** [US/US]; 5775 Morehouse Drive, San Diego, California 92121 (US). **DONDETI, Lakshminath Reddy** [IN/US]; 5775 Morehouse Drive, San Diego, California 92121 (US).

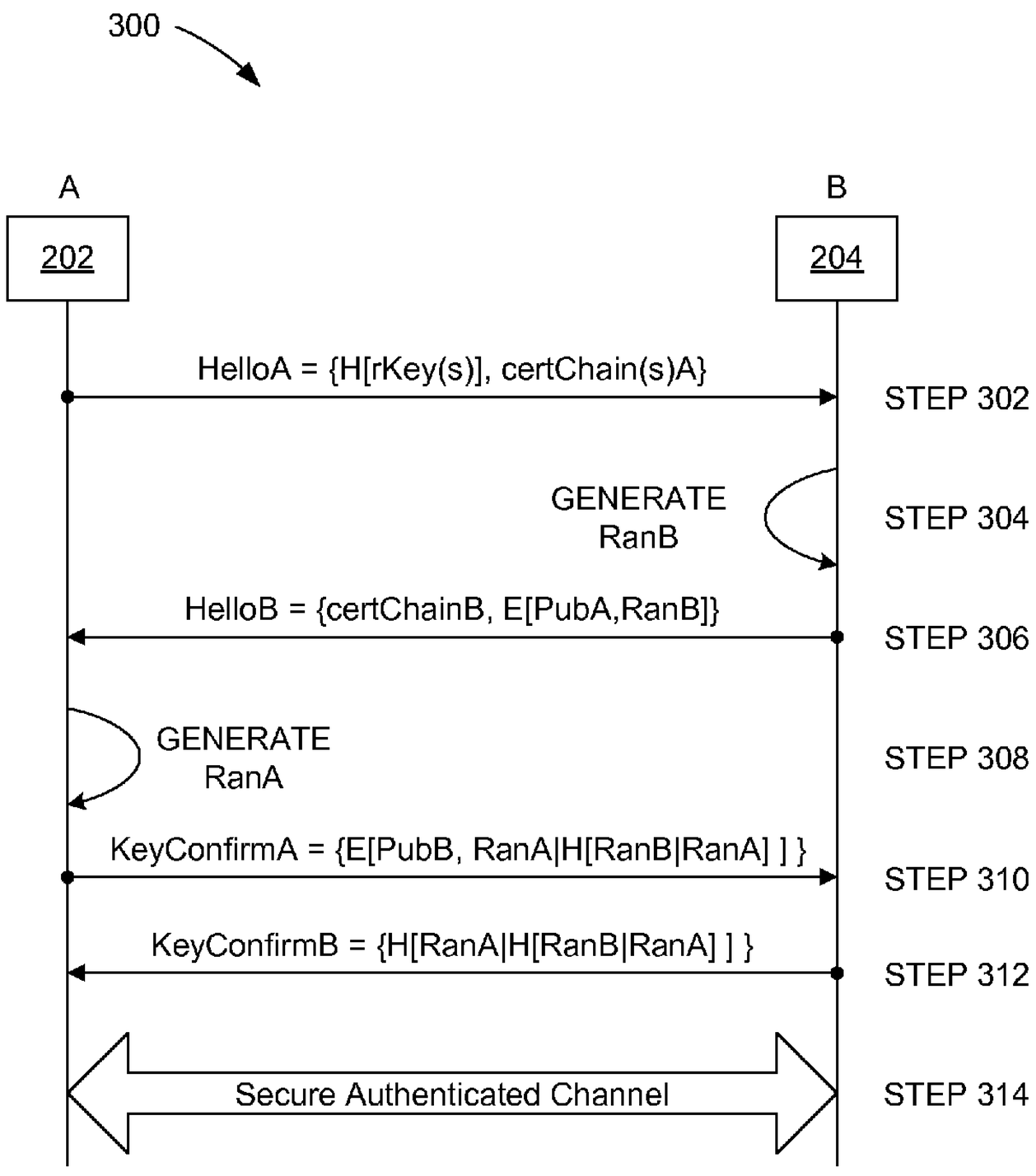
(74) Agent: **BACHAND, Richard A.**; 5775 Morehouse Drive, San Diego, California 92121 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL,

*[Continued on next page]*

(54) Title: METHOD AND APPARATUS FOR MUTUAL AUTHENTICATION




**(57) Abstract:** Disclosed is a method for mutual authentication between a station, having a digital rights agent, and a secure removable media device. The digital rights agent initiates mutual authentication by sending a message to the secure removable media device. The secure removable media device encrypts a first random number using a public key associated with the digital rights agent. The digital rights agent decrypts the encrypted first random number, and encrypts a second random number and a first hash based on at least the first random number. The secure removable media device decrypts the encrypted second random number and the first hash, verifies the first hash to authenticate the digital rights agent, and generates a second hash based on at least the second random number. The digital rights agent verifies the second hash to authenticate the secure removable media device.

WO 2008/045773 A3

WO 2008/045773 A3

PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Declarations under Rule 4.17:**

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

**Published:**

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

**(88) Date of publication of the international search report:**
12 June 2008

# METHOD AND APPARATUS FOR MUTUAL AUTHENTICATION

## Claim of Priority under 35 U.S.C. §119

**[0001]** The present Application for Patent claims priority to: Provisional Application No. 60/850,882, entitled "METHOD AND APPARATUS FOR MUTUAL AUTHENITICATION" filed October 10, 2006. This Provisional Application is assigned to the assignee hereof and is hereby expressly incorporated by reference herein.

## BACKGROUND

### Field

**[0002]** The present invention relates generally to wireless communications, and more specifically to mutual authentication.

### Background

**[0003]** A mobile subscriber may want to access content protected by a system which would require authentication with another entity or agent. A popular authentication protocol is the Internet Key Exchange (IKE) protocol, described in RFC 4306. However, the IKE protocol assumes that the entities in the authentication process have enough computing or processing power such that the speed of the authentication is not a concern.

**[0004]** There is therefore a need in the art for technique for efficient mutual authentication with a device having limited processing power.

## SUMMARY

**[0005]** An aspect of the present invention may reside in a method for mutual authentication between a first entity and a second entity. In the method, the first entity initiates mutual authentication by sending a message to the second entity. The second entity verifies a first public key associated with the first entity, generates a first random number, encrypts the first random number using the first public key, and sends the encrypted first random number in a message to the first entity. The first entity verifies a

second public key associated with the second entity, decrypts the encrypted first random number using a first private key corresponding to the first public key, generates a second random number, generating a first hash based on at least the first random number, encrypts the second random number and the first hash using the second public key, and sends the encrypted second random number and first hash in a message to the second entity. The second entity decrypts the encrypted second random number and first hash using a second private key corresponding to the second public key, verifies the first hash to authenticate the first entity, generates a second hash based on at least the second random number, and sends the second hash to the first entity. The first entity verifies the second hash to authenticate the second entity.

**[0006]** In more detailed aspects of the invention, the first entity and the second entity each derive a session encryption key and message authentication code (MAC) key using the first random number and the second random number based on a key derivation function, for use in communications between the first entity and the second entity.

**[0007]** Additionally, the message initiating mutual authentication may include a hash of at least one trusted root key and a corresponding certificate chain for the first entity. The certificate chain for the first entity may include the public key associated with the first entity. Also, the message from the second entity to the first entity having the encrypted first random number further may include a certificate chain for the second entity. The certificate chain for the second entity may include the public key associated with the second entity.

**[0008]** In other more detailed aspects of the invention, the first entity may be a digital rights agent of a mobile station, and the second entity may be a secure removable media device. The second entity may have limited processing power. Also, the first hash may be further based on the second random number such that the first hash is generated based on the first random number concatenated with the second random number. The second hash may be further based the first random number, or further based on the first hash such that the second hash may be based on the second random number concatenated with the first hash.

**[0009]** Another aspect of the invention may reside in an apparatus for mutual authentication including means for initiating mutual authentication, means for verifying a first public key, generating a first random number, and encrypting the first random number using the first public key, means for verifying a second public key, decrypting

the encrypted first random number using a first private key corresponding to the first public key, generating a second random number, generating a first hash based on at least the first random number, and encrypting the second random number and the first hash using the second public key, means for decrypting the encrypted second random number and first hash using a second private key corresponding to the second public key, verifying the first hash for authentication, and generating a second hash based on at least the second random number, and means for verifying the second hash for authentication.

**[0010]** Another aspect of the invention may reside in a mobile station having mutual authentication with a secure removable media device, and including a digital rights agent. The digital rights agent initiates mutual authentication by sending a message to a secure removable media device, wherein the secure removable media device verifies a first public key associated with the digital rights agent, generates a first random number, encrypts the first random number using the first public key, and sends the encrypted first random number in a message to the digital rights agent. The digital rights agent verifies a second public key associated with the secure removable media device, decrypts the encrypted first random number using a first private key corresponding to the first public key, generates a second random number, generates a first hash based on at least the first random number, encrypts the second random number and the first hash using the second public key, and sends the encrypted second random number and first hash in a message to the secure removable media device, wherein the secure removable media device decrypts the encrypted second random number and first hash using a second private key corresponding to the second public key, verifies the first hash to authenticate the digital rights agent, generates a second hash based on at least the second random number, and sends the second hash to the digital rights agent. The digital rights agent verifies the second hash to authenticate the secure removable media device.

**[0011]** Yet another aspect of the invention may reside is computer program product comprising computer readable medium comprising code for causing a computer of a station having a digital rights agent to initiate mutual authentication by sending a message to a secure removable media device, wherein the secure removable media device verifies a first public key associated with the digital rights agent, generates a first random number, encrypts the first random number using the first public key, and sends

the encrypted first random number in a message to the digital rights agent, code for causing a computer to cause the digital rights agent to verify a second public key associated with the secure removable media device, decrypt the encrypted first random number using a first private key corresponding to the first public key, generate a second random number, generate a first hash based on at least the first random number, encrypt the second random number and the first hash using the second public key, and send the encrypted second random number and first hash in a message to the secure removable media device, wherein the secure removable media device decrypts the encrypted second random number and first hash using a second private key corresponding to the second public key, verifies the first hash to authenticate the digital rights agent, generates a second hash based on at least the second random number, and sends the second hash to the digital rights agent, and code for causing a computer to cause the digital rights agent to verify the second hash to authenticate the secure removable media device.

**[0012]** Another aspect of the invention may reside in a computer program product, comprising computer readable medium comprising code for causing a computer to cause a secure removable media device to verify a first public key associated with a digital rights agent, generate a first random number, encrypt the first random number using the first public key, and send the encrypted first random number in a message to the digital rights agent, wherein the digital rights agent verifies a second public key associated with the secure removable media device, decrypts the encrypted first random number using a first private key corresponding to the first public key, generates a second random number, generates a first hash based on at least the first random number, encrypts the second random number and the first hash using the second public key, and sends the encrypted second random number and first hash in a message to the secure removable media device, and code for causing a computer to cause the secure removable media device to decrypt the encrypted second random number and first hash using a second private key corresponding to the second public key, verify the first hash to authenticate the digital rights agent, generate a second hash based on at least the second random number, and send the second hash to the digital rights agent, wherein the digital rights agent verifies the second hash to authenticate the secure removable media device.

## BRIEF DESCRIPTION OF THE DRAWINGS

**[0013]** Figure 1 is an example of a wireless communication system;

**[0014]** Figure 2 is a block diagram of a mobile station and a secure removable media device having mutual authentication;

**[0015]** Figure 3 is a flow diagram of a method for mutual authentication between a mobile station and a secure removable media device.

## DETAILED DESCRIPTION

**[0016]** The word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any embodiment described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments.

**[0017]** A remote station, also known as a mobile station (MS), an access terminal (AT), user equipment or subscriber unit, may be mobile or stationary, and may communicate with one or more base stations, also known as base transceiver stations (BTSs) or node Bs. A remote station transmits and receives data packets through one or more base stations to a base station controller, also known as radio network controllers (RNCs). Base stations and base station controllers are parts of a network called an access network. An access network transports data packets between multiple remote stations. The access network may be further connected to additional networks outside the access network, such as a corporate intranet or the Internet, and may transport data packets between each remote station and such outside networks. A remote station that has established an active traffic channel connection with one or more base stations is called an active remote station, and is said to be in a traffic state. A remote station that is in the process of establishing an active traffic channel connection with one or more base stations is said to be in a connection setup state. A remote station may be any data device that communicates through a wireless channel. A remote station may further be any of a number of types of devices including but not limited to PC card, compact flash, external or internal modem, or wireless phone. The communication link through which the remote station sends signals to the base station is called an uplink, also known as a reverse link. The communication link through which a base station sends signals to a remote station is called a downlink, also known as a forward link.

**[0018]** With reference to Figure 2, a wireless communication system 100 includes one or more wireless mobile stations (MS) 102, one or more base stations (BS) 104, one or

more base station controllers (BSC) 106, and a core network 108. Core network may be connected to an Internet 110 and a Public Switched Telephone Network (PSTN) 112 via suitable backhauls. A typical wireless mobile station may include a handheld phone, or a laptop computer. Wireless communication system 100 may employ any one of a number of multiple access techniques such as code division multiple access (CDMA), time division multiple access (TDMA), frequency division multiple access (FDMA), space division multiple access (SDMA), polarization division multiple access (PDMA), or other modulation techniques known in the art.

**[0019]** Many low cost devices with limited computing power are being introduced into the market such as smart cards and flash memory (in many different form factors). Such devices may require authentication. For example, there is a desire to have these devices hold rights for use with Digital Rights Management (DRM) systems. Before exchanging rights with these devices, there should be mutual authentication of both entities involved in the exchange to limit the exchange to authorized entities. These embodiments provide an efficient method to accomplish the mutual authentication, and also provide a confirmed exchange of a secret that can be used in further communicates between the involved entities. The efficiency is both in terms of computing power and speed.

**[0020]** As apparent to one skilled in the art, the mutual authentication schemes can be used anytime mutual authentication between two entities is required. The mutual authentication schemes are not limited to the specific applications (such a Digital Rights Management), systems, and devices used here to describe the embodiments.

**[0021]** One embodiment of the invention performs a mutual authentication with a confirmed key exchange using the exchange of 4 messages. It requires 2 public key signature verifications (+ 1 for every intermediate certificate), 2 public key encryptions, 2 public key decryptions, 2 hash generations and 2 hash verifications. The specific number of message exchanges, public key verifications, public key decryptions, hash generations, and hash verifications may be split or altered to achieved required amounts of security and efficiency.

**[0022]** The efficiency of the protocol is enhanced by minimizing the number of public key cryptographic operations and using hash functions to provide proof of possession of the exchanged key material.

**[0023]** An efficient mutual authentication and confirmed key exchange protocol is described for use with compute-bound devices. The efficiency is accomplished by

minimizing the number of public key operations and using cryptographic hashes to provide proof of possession.

**[0024]** The protocol is illustrated with respect to Figures 2 and 3 showing a method 300 (Figure 3) for mutual authentication. The steps below correspond to the numbered arrows in the Figure 3.

**[0025]** In the method 300, Entity A, e.g., a DRM agent 202 of the MS 102, sends the HelloA message (step 302) to entity B, e.g., a secure removable media (SRM) device 204 having an SRM agent 206. The SRM agent manages access to secure storage 208 in the SRM device. (An operating system 210 of the MS may directly access general storage 212 of the SRM device.) HelloA consists of hashes of the trusted Root Keys (or the Root Keys themselves) and the corresponding certificate chains. Upon receiving this message, entity B finds a Root Key it trusts from the message and finds a certificate chain under the selected Root Key. It verifies entity A's certificate chain under the selected Root Key.

**[0026]** Entity B generates a random number RanB (step 304).

**[0027]** Entity B sends the HelloB message to entity A (step 306). HelloB consists of B's certificate chain under the selected Root Key and along with RanB encrypted with entity A's public key from the certificate chain selected after step 302. Upon receiving this message, entity A verifies entity B's certificate chain. If valid, it decrypts RanB with its private key (corresponding to the selected Root Key).

**[0028]** Note that once the Root Key selection and certificate chain exchange has occurred, entity A and entity B will have each other's certificate chain. Thus, these parameters may not need to be sent between entity A and entity B in future HelloA and HelloB messages for a future mutual authentication. In that case, the certificate chain exchange in steps 302 and 306 may be optional.

**[0029]** Entity A generates RanA (step 308).

**[0030]** Entity A sends the KeyConfirmA message to entity B (step 310). KeyConfirmA consists of RanA concatenated with the hash of RanB concatenated with RanA (H[RanA | RanB]) and all this encrypted with B's public key. Upon receiving this message, entity B decrypts it. Using the decrypted RanA, it verifies the hash of RanB concatenated with RanA. Note: at this step, entity B has authenticated entity A and is assured that entity A knows RanB.

**[0031]** Entity B sends the KeyConfirmB message to entity A (step 312). KeyConfirmB consists of the hash of the decrypted portion of the KeyConfirmA message. Upon receiving this message, entity A verifies the hash. Note: at this step, entity A has authenticated entity B and is assured that entity B knows RanA.

**[0032]** At this point, both entities have authenticated each other and have confirmed that they each share the same RanA and RanB. RanA and RanB can now be used to derive a session encryption key (SK) and a MAC key (MK) based on a Key Derivation Function (KDF) for use with further communications between the parties (step 314).

**[0033]** The messages details are given below. The HelloA message is sent to initiate the mutual authentication with key confirmation protocol. The Hello A has a "version" parameter and a "rootAndChains[ ]" parameter. The version parameter may be an 8 bit value that contains the protocol version of this message. It is mapped as the 5 MSBs for the major version and the 3 LSBs for the minor version. The rootAndChains[ ] parameter may be an array of the root hashes and certificate chains for entity A under all the trust models supported by A. The structure for the parameter, RootHashAndCertChain is a parameter rootHash, which is the SHA-1 hash of the trust model's root public key, and a parameter certChain, the entity's certificate chain under the root public key. The entity's certificate comes first followed by any CA certificates (in order of signing) up to but not including the root certificate.

**[0034]** The HelloB message continues the mutual authentication with key confirmation protocol by entity B. The following table describes the parameters. The HelloB has the parameters: "version", "status", "certChain", and "encRanB". The version parameter may be an 8 bit value that contains the protocol version of this message. It is mapped as the 5 MSBs for the major version and the 3 LSBs for the minor version. The status parameter may be an 8 bit value that contains the status of entity B processing the HelloA message. Values for the status parameter may be 0 for success - no error were encountered with the previous message, and 1 for noSharedRootKey - entity B did not find a root key that it shares with entity A. Values 2-255 may be reserved for future use. The certChain parameter is entity B's certificate chain under a root key selected from the HelloA message. If the value of the status parameter is not success, the certChain parameter is not present. The encRanB parameter is an RSA-OAEP encrypted ranB, using the public key of entity A (from the selected certificate chain).

ranB may be 20 byte random number generated by entity B. If the value of status is not success, the encRanB parameter is not present.

**[0035]** The KeyConfirmA message continues the mutual authentication with key confirmation protocol by entity A. The KeyConfirmA message has a "version" parameter and a "encRanB" parameter. The version parameter may be an 8 bit value that contains the protocol version of this message. It may be mapped as the 5 MSBs for the major version and the 3 LSBs for the minor version. The encRanB parameter may be an RSA-OAEP encrypted KeyConfirmData structure having a "ranA" parameter and a "hashBA" parameter. The ranA parameter may be a 20-byte random number generated by entity A, and the hash BA parameter may be the SHA-1 hash of ranB concatenated with ranA.

**[0036]** The KeyConfirmB message finalizes the mutual authentication with key confirmation protocol by entity B. The KeyConfirmB message has a "version" parameter, a status parameter, and a "hashKeyConfirm" parameter. The version parameter may be an 8 bit value that contains the protocol version of this message. It may be mapped as the 5 MSBs for the major version and the 3 LSBs for the minor version. The status parameter may be an 8 bit value that contains the status of entity B processing the message. The hashKeyConfirm parameter may be the SHA-1 hash of the KeyConfirmData structure that was decrypted by entity B. If the value of the status parameter is not success, this parameter is not present.

**[0037]** Another aspect of the invention may reside in a mobile station 102 including a control processor 216 and the OS 210 for causing the DRM agent 202 to implement the method 300. Yet another aspect of the invention may reside in a computer program product comprising computer readable medium (such as a memory device 218) comprising code for causing a computer to cause the DRM agent to perform the steps of the method 300.

**[0038]** Those of skill in the art would understand that information and signals may be represented using any of a variety of different technologies and techniques. For example, data, instructions, commands, information, signals, bits, symbols, and chips that may be referenced throughout the above description may be represented by voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, or any combination thereof.

**[0039]** Those of skill would further appreciate that the various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the embodiments disclosed herein may be implemented as electronic hardware, computer software, or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, modules, circuits, and steps have been described above generally in terms of their functionality. Whether such functionality is implemented as hardware or software depends upon the particular application and design constraints imposed on the overall system. Skilled artisans may implement the described functionality in varying ways for each particular application, but such implementation decisions should not be interpreted as causing a departure from the scope of the present invention.

**[0040]** The various illustrative logical blocks, modules, and circuits described in connection with the embodiments disclosed herein may be implemented or performed with a general purpose processor, a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general purpose processor may be a microprocessor, but in the alternative, the processor may be any conventional processor, controller, microcontroller, or state machine. A processor may also be implemented as a combination of computing devices, e.g., a combination of a DSP and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration.

**[0041]** The steps of a method or algorithm described in connection with the embodiments disclosed herein may be embodied directly in hardware, in a software module executed by a processor, or in a combination of the two. A software module may reside in RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, or any other form of storage medium known in the art. An exemplary storage medium is coupled to the processor such the processor can read information from, and write information to, the storage medium. In the alternative, the storage medium may be integral to the processor. The processor and the storage medium may reside in an ASIC. The ASIC

may reside in a user terminal. In the alternative, the processor and the storage medium may reside as discrete components in a user terminal.

**[0042]** In one or more exemplary embodiments, the functions described may be implemented in hardware, software, firmware, or any combination thereof. If implemented in software as a computer program product, the functions may be stored on or transmitted over as one or more instructions or code on a computer-readable medium. Computer-readable media includes both computer storage media and communication media including any medium that facilitates transfer of a computer program from one place to another. A storage media may be any available media that can be accessed by a computer. By way of example, and not limitation, such computer-readable media can comprise RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium that can be used to carry or store desired program code in the form of instructions or data structures and that can be accessed by a computer. Also, any connection is properly termed a computer-readable medium. For example, if the software is transmitted from a website, server, or other remote source using a coaxial cable, fiber optic cable, twisted pair, digital subscriber line (DSL), or wireless technologies such as infrared, radio, and microwave, then the coaxial cable, fiber optic cable, twisted pair, DSL, or wireless technologies such as infrared, radio, and microwave are included in the definition of medium. Disk and disc, as used herein, includes compact disc (CD), laser disc, optical disc, digital versatile disc (DVD), floppy disk and blu-ray disc where disks usually reproduce data magnetically, while discs reproduce data optically with lasers. Combinations of the above should also be included within the scope of computer-readable media.

**[0043]** The previous description of the disclosed embodiments is provided to enable any person skilled in the art to make or use the present invention. Various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments without departing from the spirit or scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown herein but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.

# CLAIMS

1. A method for mutual authentication between first entity and a second entity; comprising:

the first entity initiating mutual authentication by sending a message to the second entity;

the second entity verifying a first public key associated with the first entity, generating a first random number, encrypting the first random number using the first public key, and sending the encrypted first random number in a message to the first entity;

the first entity verifying a second public key associated with the second entity, decrypting the encrypted first random number using a first private key corresponding to the first public key, generating a second random number, generating a first hash based on at least the first random number, encrypting the second random number and the first hash using the second public key, and sending the encrypted second random number and first hash in a message to the second entity;

the second entity decrypting the encrypted second random number and first hash using a second private key corresponding to the second public key, verifying the first hash to authenticate the first entity, generating a second hash based on at least the second random number, and sending the second hash to the first entity; and

the first entity verifying the second hash to authenticate the second entity.

2. A method for mutual authentication as defined in claim 1, wherein the first entity and the second entity each derive a session encryption key and message authentication code (MAC) key using the first random number and the second random number based on a key derivation function, for use in communications between the first entity and the second entity.

3. A method for mutual authentication as defined in claim 1, wherein the message initiating mutual authentication includes a hash of at least one trusted root key and a corresponding certificate chain for the first entity.

4. A method for mutual authentication as defined in claim 1, wherein the message from the second entity to the first entity having the encrypted first random number further includes a certificate chain for the second entity.

5. A method for mutual authentication as defined in claim 1, wherein the first entity is a digital rights agent and the second entity is a secure removable media device.

6. A method for mutual authentication as defined in claim 1, wherein the first entity is a mobile station.

7. A method for mutual authentication as defined in claim 1, wherein the second entity has limited processing power.

8. A method for mutual authentication as defined in claim 1, wherein the first hash is further based on at least the second random number such that the first hash is generated based on at least the first random number concatenated with the second random number.

9. A method for mutual authentication as defined in claim 1, wherein the second hash is further based on at least the first random number.

10. A method for mutual authentication as defined in claim 1, wherein the second hash is further based on at least the first hash such that the second hash is generated based on at least the second random number concatenated with the first hash.

11. Apparatus for mutual authentication comprising:

means for initiating mutual authentication;

means for verifying a first public key, generating a first random number, and encrypting the first random number using the first public key;

means for verifying a second public key, decrypting the encrypted first random number using a first private key corresponding to the first public key, generating a second random number, generating a first hash based on at least the first random

number, and encrypting the second random number and the first hash using the second public key;

means for decrypting the encrypted second random number and first hash using a second private key corresponding to the second public key, verifying the first hash for authentication, and generating a second hash based on at least the second random number; and

means for verifying the second hash for authentication.

12. Apparatus for mutual authentication as defined in claim 11, further comprising means for deriving a session encryption key and message authentication code (MAC) key using the first random number and the second random number based on a key derivation function, for use in communications between the first entity and the second entity.

13. Apparatus for mutual authentication as defined in claim 11, wherein the first hash is further based on at least the second random number such that the first hash is generated based on at least the first random number concatenated with the second random number.

14. Apparatus for mutual authentication as defined in claim 11, wherein the second hash is further based on at least the first random number.

15. Apparatus for mutual authentication as defined in claim 11, wherein the second hash is further based on the first hash such that the second hash is generated based on the second random number concatenated with the first hash.

16. A station having mutual authentication with a secure removable media device, comprising:

a digital rights agent, wherein:

the digital right agent initiates mutual authentication by sending a message to the secure removable media device, wherein the secure removable media device verifies a first public key associated with the digital rights agent, generates a first random number,

encrypts the first random number using the first public key, and sends the encrypted first random number in a message to the digital rights agent;

the digital rights agent verifies a second public key associated with the secure removable media device, decrypts the encrypted first random number using a first private key corresponding to the first public key, generates a second random number, generates a first hash based on at least the first random number, encrypts the second random number and the first hash using the second public key, and sends the encrypted second random number and first hash in a message to the secure removable media device, wherein the secure removable media device decrypts the encrypted second random number and first hash using a second private key corresponding to the second public key, verifies the first hash to authenticate the digital rights agent, generates a second hash based on at least the second random number, and sends the second hash to the digital rights agent; and

the digital rights agent verifies the second hash to authenticate the secure removable media device.

17. A station having mutual authentication as defined in claim 16, wherein the digital rights agent and the secure removable media device each derive a session encryption key and message authentication code (MAC) key using the first random number and the second random number based on a key derivation function, for use in communications between the digital rights agent and the secure removable media device.

18. A station having mutual authentication as defined in claim 16, wherein the message sent by the digital rights agent to initiate mutual authentication includes a hash of at least one trusted root key and a corresponding certificate chain for the digital rights agent.

19. A station having mutual authentication as defined in claim 18, wherein the certificate chain for the digital rights agent includes the public key associated with the digital rights agent.

20. A station having mutual authentication as defined in claim 16, wherein the message sent by the secure removable media device to the digital rights agent having the encrypted first random number further includes a certificate chain for the secure removable media device.

21. A station having mutual authentication as defined in claim 20, wherein the certificate chain for the secure removable media device includes the public key associated with the secure removable media device.

22. A station having mutual authentication as defined in claim 16, wherein the station is a mobile station.

23. A station having mutual authentication as defined in claim 16, wherein the first hash is further based on at least the second random number such that the digital right agent generates the first hash based on at least the first random number concatenated with the second random number.

24. A computer program product, comprising:

computer readable medium comprising:

code for causing a computer to cause a digital rights agent of a station to initiate mutual authentication by sending a message to a secure removable media device, wherein the secure removable media device verifies a first public key associated with the digital rights agent, generates a first random number, encrypts the first random number using the first public key, and sends the encrypted first random number in a message to the digital rights agent;

code for causing a computer to cause the digital rights agent to verify a second public key associated with the secure removable media device, decrypt the encrypted first random number using a first private key corresponding to the first public key, generate a second random number, generate a first hash based on at least the first random number, encrypt the second random number and the first hash using the second public key, and send the encrypted second random number and first hash in a message to the secure removable media device, wherein the secure removable media device decrypts

the encrypted second random number and first hash using a second private key corresponding to the second public key, verifies the first hash to authenticate the digital rights agent, generates a second hash based on at least the second random number, and sends the second hash to the digital rights agent; and

code for causing a computer to cause the digital rights agent to verify the second hash to authenticate the secure removable media device.

25. A computer program product, comprising:

computer readable medium comprising:

code for causing a computer to cause a secure removable media device to verify a first public key associated with a digital rights agent, generate a first random number, encrypt the first random number using the first public key, and send the encrypted first random number in a message to the digital rights agent, wherein the digital rights agent verifies a second public key associated with the secure removable media device, decrypts the encrypted first random number using a first private key corresponding to the first public key, generates a second random number, generates a first hash based on at least the first random number, encrypts the second random number and the first hash using the second public key, and sends the encrypted second random number and first hash in a message to the secure removable media device;

code for causing a computer to cause the secure removable media device to decrypt the encrypted second random number and first hash using a second private key corresponding to the second public key, verify the first hash to authenticate the digital rights agent, generate a second hash based on at least the second random number, and send the second hash to the digital rights agent, wherein the digital rights agent verifies the second hash to authenticate the secure removable media device.

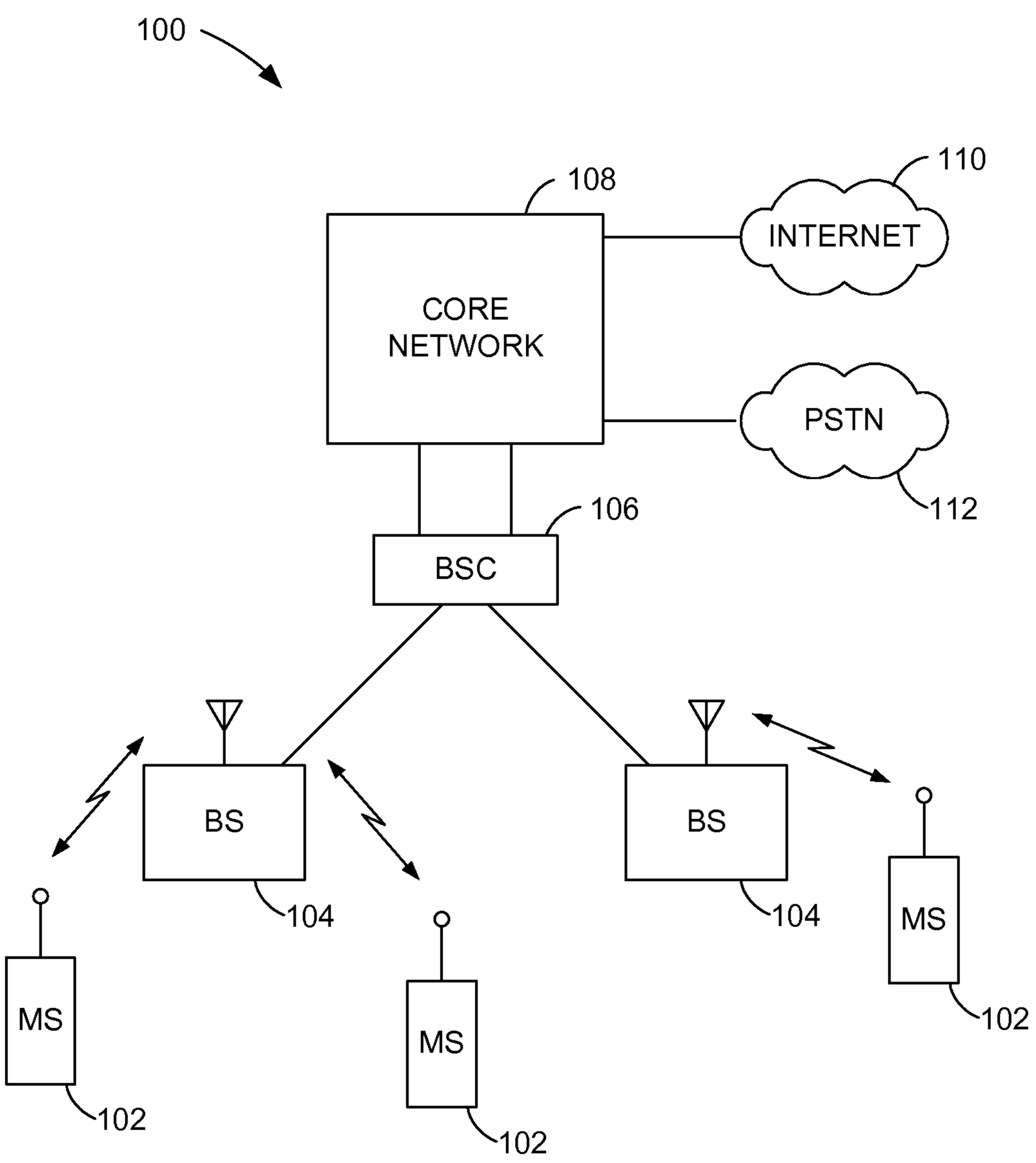
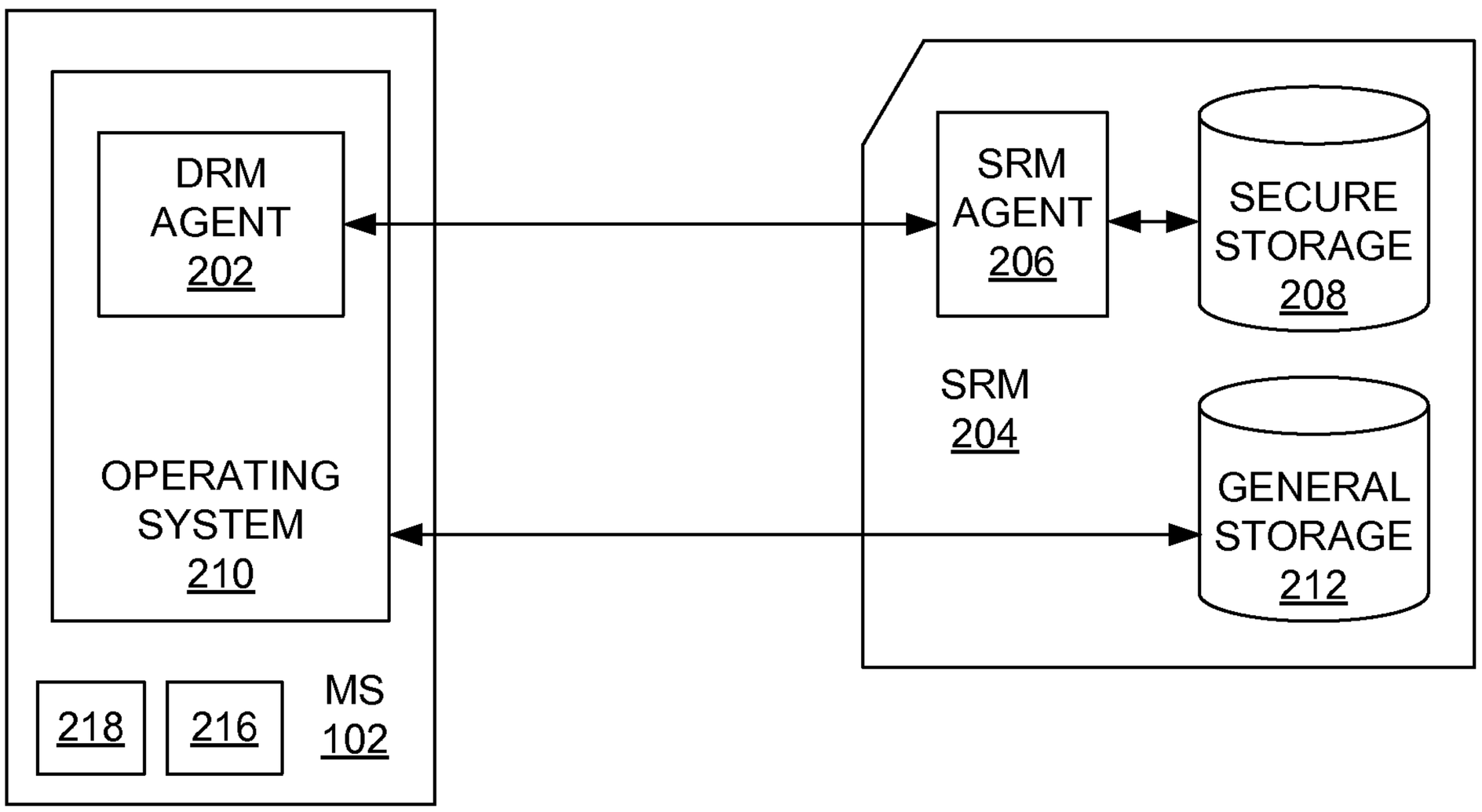

100
108
110
INTERNET
CORE NETWORK
PSTN
112
106
BSC
BS
BS
104
104
MS
MS
MS
102
102
102

FIG. 1

FIG. 2


DRM
AGENT
202
OPERATING
SYSTEM
210
218
216
MS
102
SRM
AGENT
206
SECURE
STORAGE
208
SRM
204
GENERAL
STORAGE
212

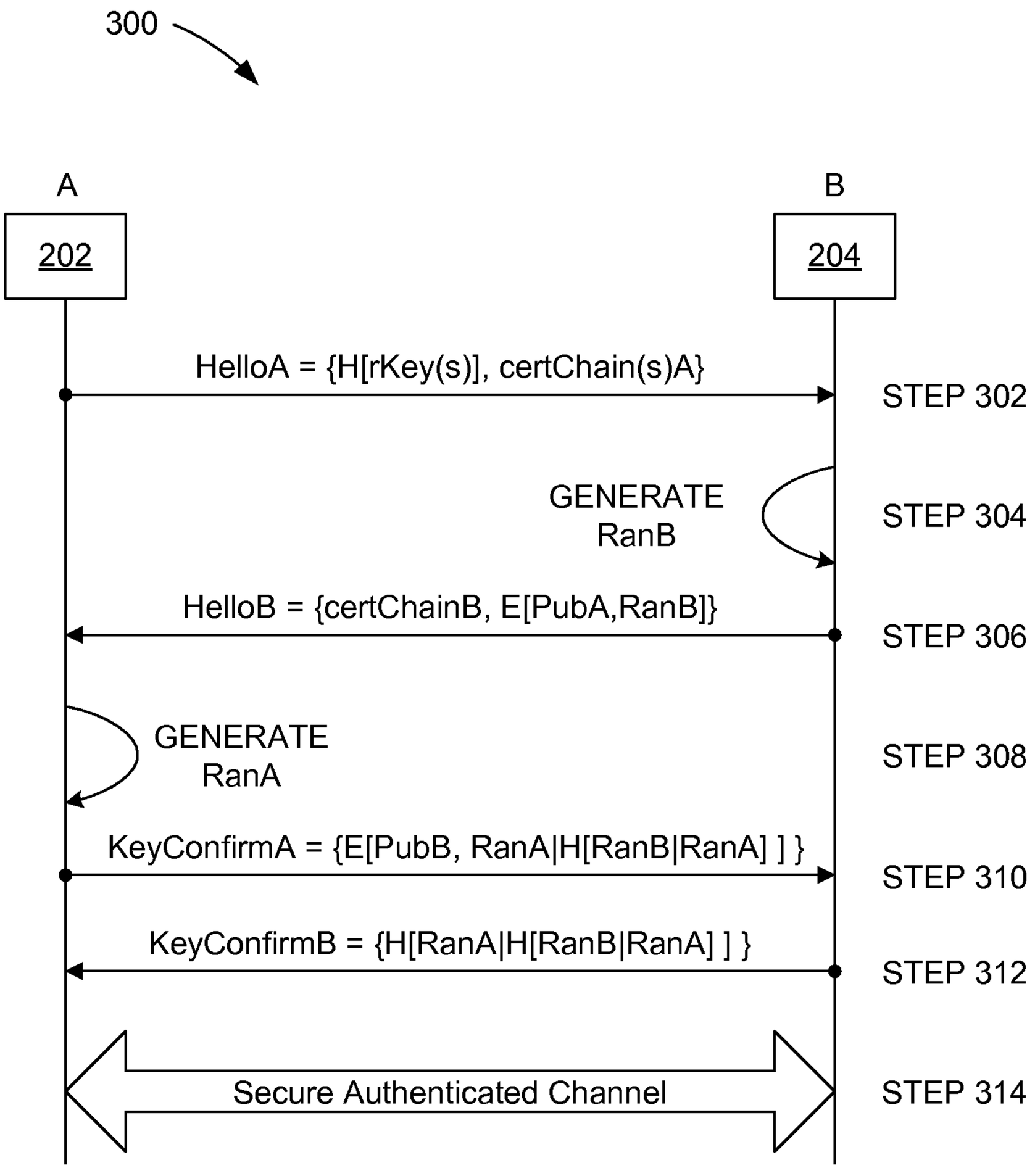
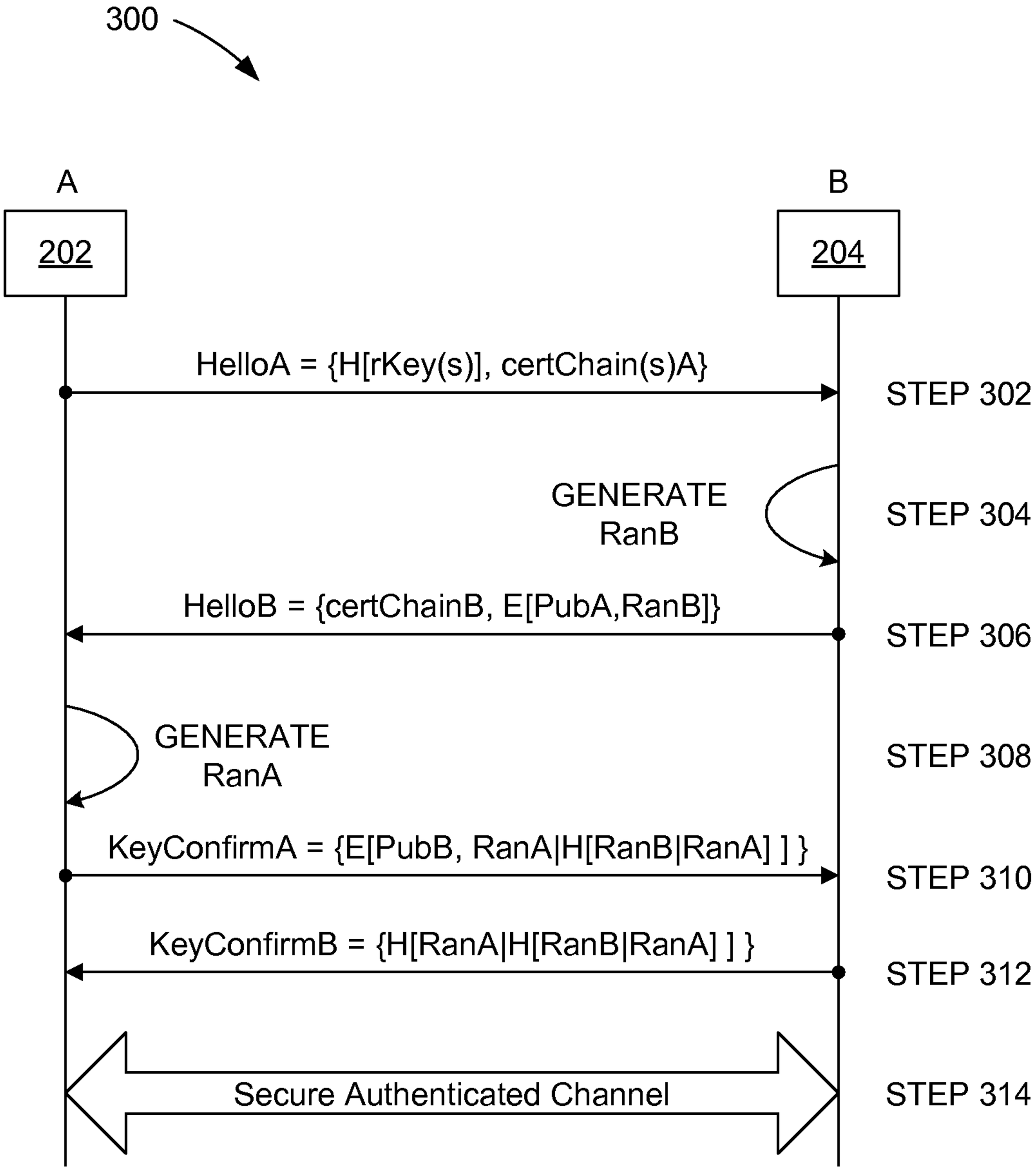

300
A
B
202
204
HelloA = {H[rKey(s)], certChain(s)A}
STEP 302
GENERATE
RanB
STEP 304
HelloB = {certChainB, E[PubA,RanB]}
STEP 306
GENERATE
RanA
STEP 308
KeyConfirmA = {E[PubB, RanA|H[RanB|RanA] ] }
STEP 310
KeyConfirmB = {H[RanA|H[RanB|RanA] ] }
STEP 312
Secure Authenticated Channel
STEP 314

FIG. 3


300
A
202
B
204
HelloA = {H[rKey(s)], certChain(s)A}
STEP 302
GENERATE
RanB
STEP 304
HelloB = {certChainB, E[PubA,RanB]}
STEP 306
GENERATE
RanA
STEP 308
KeyConfirmA = {E[PubB, RanA|H[RanB|RanA] ] }
STEP 310
KeyConfirmB = {H[RanA|H[RanB|RanA] ] }
STEP 312
Secure Authenticated Channel
STEP 314